Are You Ready for the New Face of Law Enforcement?
Facial Recognition Technology

by

Captain Rob Castro
Glendora Police Department

September 2009

COMMAND COLLEGE CLASS 45

The Command College Futures Study Project is a FUTURES study of a particular emerging issue of relevance to law enforcement. Its purpose is NOT to predict the future; rather, to project a variety of possible scenarios useful for strategic planning in anticipation of the emerging landscape facing policing organizations.

This journal article was created using the futures forecasting process of Command College and its outcomes. Defining the future differs from analyzing the past, because it has not yet happened. In this article, methodologies have been used to discern useful alternatives to enhance the success of planners and leaders in their response to a range of possible future environments.

Managing the future means influencing it—creating, constraining and adapting to emerging trends and events in a way that optimizes the opportunities and minimizes the threats of relevance to the profession.

The views and conclusions expressed in the Command College Futures Project and journal article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).

Are You Ready for the New Face of Law Enforcement, Facial Recognition Technology?

Do you have a face only law enforcement would love; love to arrest, that is? On the pages that follow, we will look at the development and use of an emerging technology to instantly identify individuals through facial recognition technologies for law enforcement. The question is: how will facial recognition technology will affect suspect apprehension for California municipal police departments in the future? It could solve many of the current deficiencies concerning the identification of individuals, and allow the police to be able to patrol neighborhoods, crowded entertainment venues and transportation hubs with the ability to identify any person of interest. This technology may the primary method of personal identification verification of the future.

The Current State of Security

Security is a major concern for Americans and many other developed countries. Threats to American security have come from within our borders and from abroad. Many protective measures are being used to enhance public safety, especially in the wake of the terrorist attacks of September 11, 2001. Since that time, Americans have become keenly aware that improved security measures are necessary to reduce the opportunity for large scale attacks on our soil. To that end, government and private business officials have been working to develop improved security systems to identify and control the movement of known individuals who are a threat to our security[1]. As a part of this work, airports, casinos, and departments of motor vehicles have been testing various systems including facial recognition to improve security and personal identification.

California is one of the most populous states in America. The density of population, coupled with the large number of visitors coming to California every year presents unique challenges to California law enforcement and necessitates the ability to effectively locate and apprehend dangerous and wanted persons. For the western United States California law enforcement agencies have traditionally led the way for the application of new technologies to public safety. Facial recognition technology may have many benefits to assist law enforcement to instantly identify criminals as well as enhance financial security and providing convenience to everyday tasks. This same technology could be applied to enhancing our personal security by confirming identity when conducting online business over the internet, making a withdrawal from an ATM machine, or signing on to a secure computer. Imagine the fraud that could be eliminated if a more secure form of identification was readily available.

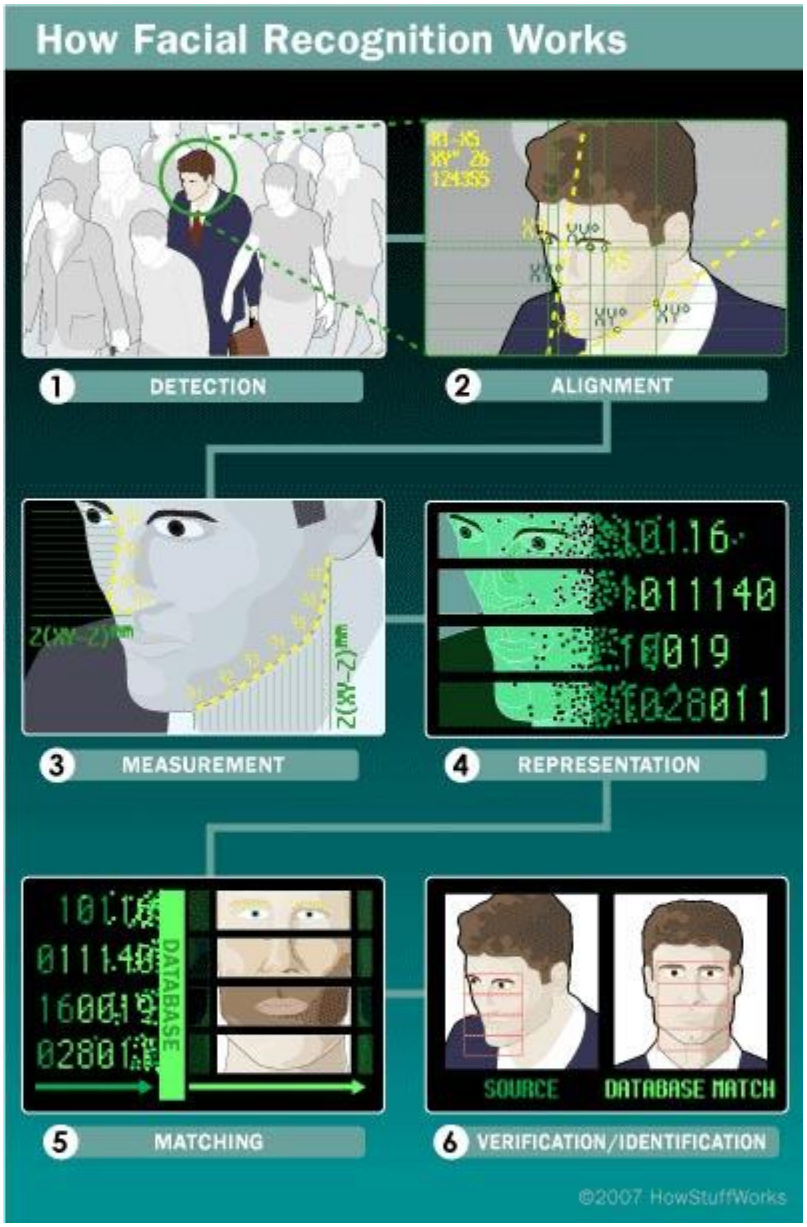
Contemporary identification systems commonly use biometric technology to confirm the identity of an individual for a variety of purposes. Biometrics identifies and measures unique biological and psychological features of individuals for the purpose of identification and verification. The two major categories are physical biometrics and behavioral biometrics. Physical biometrics consists of a century-old staple of police investigations, the fingerprint. Fingerprint recognition systems use the unique characteristics of ridges and valleys that form loops, arches and swirls on the fingertips. Already in use are enhanced systems using hand geometry (which measures the unique features in the structure of the hand), iris recognition, voice recognition measures the unique patterns of an individual's voice pattern, and facial recognition examining unique facial features. On the other hand, behavioral biometrics consists of keystroke recognition to examine the unique variables an individual performs when typing on a computer keyboard and signature recognition to examine the manner in which an individual signs their name.

For any biometric system to operate, it must have records in its database against which it can search for matches. For law enforcement purposes, this means the individual must already have had formal police contact where biometrics was captured. Facial recognition, however, is able to leverage existing photographic databases from a variety of government sources. For example, there are high quality mugshots of criminals in the Los Angeles County Regional Identification System (LACRIS). The LACRIS Mugshot System is a technically advanced system that provides mugshots of each arrested individual and is accessible to police officers throughout Los Angeles County. It includes an Intranet web application that permits searches, creation of mugbooks, and composition of "six pack lineups." Additional functionality is available on dedicated terminals at 14 strategically located remote sites which are accessible to all police agencies. Four sites include the ability to conduct facial recognition matching. The Mugshot System is integrated with Cal-Photo, which establishes a statewide network of mugshot and DMV photos. Similarly, facial recognition is often able to utilize existing surveillance system database such as surveillance cameras or closed circuit television (CCTV). [2]

How Facial Recognition Works

Facial recognition compares the three-dimensional geometry of the human face against the three-dimensional image of the database photographs utilizing computer algorithms.[3] Current limitations in facial recognition systems do not allow for accurate scanning of a moving subject. Present systems are effective in controlled environments such as an airport security check point or DMV office. As with any technology systems, rapid system improvements are occurring that will allow for field use by police officers.   The global efforts in biometric development will mean that many current limitations will be resolved and biometric technology, including facial recognition, will become increasingly common as a global means of controlling immigration and identifying wanted individuals.[4]

Facial recognition programs are computer based security systems that are able to automatically detect and identify human faces. These systems depend on a recognition algorithm, such as eigenface.[5] Eigenfaces are a set of eigenvectors used by the computer program to identify and classify a human face. Basically, eigenfaces are a set of standardized facial templates derived from statistical analysis of many facial pictures. The facial recognition system translates the templates into a unique code. This coding gives each template a set of numbers to represent the features on a subjects' face. Live images are compared against the eigenface templates to determine if there is a match in the system database. Figure 1 below depicts the basic steps a facial recognition system performs while conducting an analysis.



In January 2009, the FBI released a detailed study of the advancements in biometric systems and how the bureau might use this technology to identify individuals in the future. The assessment is part of the State-of-the–Art Biometrics Excellence Roadmap (SABER), an FBI initiative to plan and implement the biometric technology. “The results of the SABER study represents an important plank in our biometric efforts, one that will help us strategically prioritize the FBI’s biometric research and funding activities. As we move forward, it is critical to ensure a coordinated effort across our law enforcement community to effectively harness the benefits of emerging biometric technologies to support our nation's law enforcement and intelligence missions", said Louis Grever, Executive Director of the FBI Science and Technology Branch.[6]

Can This Technology Benefit Law Enforcement?

The use of facial recognition technology could allow officers to quickly scan individuals as police units are patrolling. Currently, automatic license plate readers are installed in many police units and automatically scan hundreds of vehicle license plates as officers patrol streets and parking lots. This technology has resulted in a significant increase in the number of stolen and wanted vehicles being located. Facial recognition technology could integrate into this existing system and allow for the scanning of individuals using mobile unit cameras and fixed cameras at public venues.

Future law enforcement applications of facial recognition technology could allow officers using handheld devices to scan an individual who has been detained and does not have identification to determine if they are wanted or can be positively identified. This type of rapid identification could result in the removal of many wanted individuals from free society and control individuals who have restrictions such as registered sex offenders or restraining orders that restrict the areas where they can be. It is accomplished by capturing a facial image via scanning a photograph or using a camera to capture a live image. The facial image is analyzed using software that measures the spatial geometry of the facial features creating a generated template. The generated template of the subject's face is compared to faces in the database to determine if there is a match. If facial recognition is used for verification purposes, the software will compare the generated template with a verified template of the claimed identity. If the system detects a match the user is notified and provided a percentage of match probability. Additional identity verification can then be applied to confirm or deny the identity match. If a match is detected through facial recognition then verification will be verified through traditional biometrics such as fingerprints. This is not a far-term forecast of usefulness; in fact, a number of agencies are already using this technology to aid in their work.

Currently, the Nevada Department of Motor Vehicles is using facial recognition to check individuals applying for drivers' licenses. The Indiana Bureau of Motor Vehicles has installed facial recognition technology at all 140 of its branches. Dell Computer currently manufacturers sixteen new laptops that offer the optional feature of the biometric facial recognition security log on. This system uses a webcam and password to ensure only the authorized user can log on to the computer. More than 20 states use facial recognition systems as a screen process for people applying for driver's licenses or identification card.[7] The integration of facial recognition technology into existing surveillance and camera systems could increase the effectiveness of law enforcement identifying wanted individuals. The issue at hand, though, may be the willingness of courts and our legislatures to allow the widespread use of facial recognition.

What Are the Legal Implications?

A question that arises when considering facial recognition technology is whether it violates legally protected privacy rights. Although the words "right to privacy" do not appear in the U.S. Constitution, the concern with protecting citizens against government intrusions in their private sphere is reflected in many of the Constitution's provisions. For example, the First Amendment protects freedom of expression and association as well as the free exercise of religion. The Fourth Amendment protects against unreasonable searches and seizures. The constitutional “right to privacy” therefore reflects concerns not only for one's physical privacy (the idea that government agents cannot barge into one's home) but also concerns less tangible interests such as the idea that citizens should be able to control certain information about themselves and to make certain decisions free of government compulsion. Moreover, the Supreme Court has cautioned that it is “not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.” (*Whalen v. Roe,* 429 U.S. 589, 605 (1977).)[8]

A sub-issue related to law enforcement use of facial recognition technology is privacy and constitutionality. Some civil libertarians argue that facial recognition is a type of mass scanning that is improper and that law enforcement must have individualized, reasonable suspicion that criminal activity is afoot before it can “search” a subject's face to see if it matches that of an individual in the database. Under current law, however, the type of facial recognition used by law enforcement to monitor public places would almost certainly be constitutional. The United States Supreme Court has explained that government action constitutes a search where it invades a person's reasonable expectation of privacy. However, the Court has found that a person does not have a reasonable expectation of privacy in those physical characteristics that are constantly exposed to the public, such as one's facial characteristics, voice, and handwriting. (*United States v. Dionisio,* 410 U.S. 1, 14 (1973).) The use of biometric facial recognition potentially implicates both types of privacy interests. In the context of law enforcement's use of biometric facial recognition to monitor public places, it does not appear that such use would violate the protections afforded by the U.S. Constitution.

The Future Application of Facial Recognition Technology to Law Enforcement

In California, law enforcement staffing is not increasing commensurate with the annual increases in population. Therefore, there is an opportunity to apply new technologies that will supplement law enforcement personnel to accomplish their mission in a more efficient and effective manner. This technology will allow for a more efficient manner of detecting wanted individuals and could result in the need for less law enforcement personnel. There are many applications for this type of technology for law enforcement, business, and consumer application.

Law enforcement leaders will need to evaluate the application of facial recognition technology and become well versed in the benefits, limitations and public concerns relating to the use of this technology. Organizations that have a clear understanding of the trends for future public safety will be in the best position to successfully implement new technologies that will enhance their effectiveness. These agencies will need a leader who can envision the future and communicate the compelling need to strategically apply technology to meet the changing policing challenges of the future. As public funding for law enforcement services continues to be reduced, the application of technology such as facial recognition could be a significant strategy to address the current demands to reduce personnel and operating costs. Facial recognition technology has the potential be a cost effective system to identify wanted individuals and improve personnel productivity. While the exact costs of a law enforcement field system are unknown at this time, application by the FBI and in the LACRIS Mugshot System have been affordable.

Conclusion

Facial recognition is by no means a perfect technology and much technical work needs to be done before it becomes a truly viable tool to counter terrorism and crime used by police officers in the field. However, the technology is getting better and there is no denying its tremendous potential. In the meantime, we as a society must decide how we want to use this new technology. By implementing reasonable safeguards, we can harness the power of the technology to maximize its public safety benefits, while minimizing the intrusion on individual privacy. Security is a growing concern globally. The application of facial recognition by law enforcement has the potential to provide an effective and non-intrusive means of enhancing security through the identification of known wanted individuals. The technology could save time by allowing officers to scan multiple individuals quickly and without the need to make physical contact as is currently the case for fingerprint comparison.

Technology is a rapidly changing part of all our personal and professional lives. We live in rapidly changing times with technology helping to improve traditional law enforcement tactics. As successful applications of facial recognition technology occur in the private sector, widespread implementation by law enforcement will quickly follow. Maintaining competence of the technological advancements and maximizing efficiency and cost savings may be the most significant challenge law enforcement will face in the future. While many law enforcement agencies have integrated computer systems and software into their law enforcement duties, the rising costs in personnel salary and benefits is limiting small and medium size police agencies from purchasing cutting edge technology. This obstacle could be overcome through resource sharing among agencies to reduce individual agency costs. Those agencies that are willing to envision the application of emerging technologies in the future and then plan and act to strategically use technology, will be in the best position to provide efficient and effective public safety in the 21st Century.

ENDNOTES

1. Biometric News and Information, 2008, [internet on-line] Available from (http://www.biometricnews.typepad.com/biometric_news_and_infrom); Internet

2. Arrison, Sonia, and Solveig Singleton. "Symposium." *Insight on the News*, (25 February 2002), 40+. Database on-line. Available from Questia, http://www.questia.com/PM.qst?a=o&d=5000711011. Internet. Accessed 11 August 2008; Internet

3. “3D Face Recognition Uses Texture and Shape of the Human Face.” *Oxford’s Science Magazine,* July 2008, 26; Internet

4. "Handing It to Biometrics." *Security Management*, February 1998, 14. Database on- line. Available from Questia, http://www.questia.com/PM.qst?a=o&d= 5002282649 Internet. Accessed 20 April 2009; Internet

5. Johnson, Ryan, and Kevin Bonsor. "How Facial Recognition Systems Work." 04 September 2001. HowStuffWorks.com. <http://electronics.howstuffworks.com/facial-recognition.htm> 14 August 2008; Internet

6. Aitoro, Jill R, “FBI studies biometrics to plan its future research.” *Nextgov,* January 1, 2009, internet, www.nextgov.com/nextgove/ng_20090113_5430.php

7. Gips, Michael A. "Assessing Trends in Access Control." *Security Management*, September 1998, 42+. Database on-line. Available from Questia, http://ww.questia.com/PM.qst?a=o&d=5002294846. Internet. Accessed 12 March 2009; Internet

8. "Information Technology Puts Privacy under Threat as Never Before." *Canadian Speeches*, May 2001, 47. Database on-line. Available from Questia, http://www.questia. com/PM.qst?a=o&d=5001028638. Internet. Accessed 16 August 2008; Internet

BIBLIOGRAPHY

Aitoro, Jill R, “FBI studies biometrics to plan its future research.” *Nextgov,* January 1, 2009, internet, www.nextgov.com/nextgove/ng_20090113_5430.php

Arrison, Sonia, and Solveig Singleton. "Symposium." *Insight on the News*, 25 February 2002, 40+. Database on-line. Available from Questia, http://www.questia.com/PM.qst?a=o&d=5000711011. Internet. Accessed 11 August 2008.

Biometric News and Information, 2008, [internet on-line] Available from http://www.biometricnews.typepad.com/biometric_news_and_infrom [08 August 2008]

Gips, Michael A. "Assessing Trends in Access Control." *Security Management*, September 1998, 42+. Database on-line. Available from Questia, http://ww.questia.com/PM.qst?a=o&d=5002294846. Internet. Accessed 11 August 2008.

"Handing It to Biometrics." *Security Management*, February 1998, 14. Database on-line. Available from Questia, http://www.questia.com/PM.qst?a=o&d= 5002282649 Internet. Accessed 11 August 2008.

"Information Technology Puts Privacy under Threat as Never Before." *Canadian Speeches*, May 2001, 47. Database on-line. Available from Questia, http://www.questia. com/PM.qst?a=o&d=5001028638. Internet. Accessed 16 August 2008.

Johnson, Ryan, and Kevin Bonsor. "How Facial Recognition Systems Work." 04 September 2001. HowStuffWorks.com. <http://electronics.howstuffworks.com/facial-recognition.htm> 14 August 2008.

Kotter, J. (1996). *Leading Change.* Boston, Massachusetts: Harvard Business School Press.